General Services Administration
Federal Acquisition Service
Pacific Rim Region

Task ID09150042
for
Information Technology (IT) and Communications Security (COMSEC)
Management Support Services

Performance Work Statement (PWS)

1.0 INTRODUCTION

1.1 Mission and Organization

The Defense Contract Audit Agency (DCAA), while serving the public interest as its primary customer, shall perform all necessary contract audits for the Department of Defense (DoD) and provide accounting and financial advisory services regarding contracts and subcontracts to all DoD components responsible for procurement and contract administration. These services shall be provided in connection with negotiation, administration, and settlement of contracts and subcontracts to ensure taxpayer dollars are spent on fair and reasonable contract prices.

The DCAA Field Detachment (DCAA-FD) performs all audits on contracts involving DoD Sensitive Compartmented Information (SCI) and Special Access Programs (SAP). DCAA also provides contract audit services to other Government agencies, as appropriate.

DCAA FD has a workforce of approximately 446 employees that are geographically dispersed across the United States. The major organizational components of DCAA-FD are its Regional Office located in Reston, VA; 16 Field Audit Offices (FAO); 4 Financial Liaison Advisor (FLA) Offices; and approximately 32 sub-offices. Many of these offices (known as Resident Offices) are located in contractors' facilities. Addresses of these Resident Offices will be provided under separate cover on an as-needed basis. Please see Appendix 2 for a list of DCAA locations by office code, city, state, zip code, and estimated number of employees.

1.2 Background

DCAAs computing infrastructure consists of laptop and desktop computers and Microsoft Windows 2008 R2 servers. The laptop and desktop computers run mostly commercial off-the-shelf (COTS) software such as Windows 7, Microsoft Office Suite, Microsoft Outlook, McAfee Anti-Virus, and Cognos Impromptu/Powerplay. Several in-house developed applications including the DCAA Management Information System (DMIS) client and the Audit Planning and Performance System (APPS) are examples of government off the shelf (GOTS). All offices connected via the DCAA network contain a Router, Switch(es), Server, and other peripherals like printers, monitors, scanners, faxes, STE's, and Multi-Function Devices (MFDs) (please refer to Appendix 3).

Additionally, DCAA-FD has a select few government systems connected via Multi-Protocol Label Switching (MPLS) circuits using high-grade link Type 1 encryption (TACLANE) devices for protection of highly sensitive information.

At the present time, DCAA has a separate contract for centralized Tier 1 Help Desk services, so any reference to "DCAA Tier 1 Help Desk" is to another contract. If the DCAA Tier 1 Help Desk is unable to resolve an IT problem remotely, the problem will be submitted via a reassignment of the trouble ticket to the Tier 2 Contractor under this task to solve.

2.0 SCOPE

This is a performance based statement of work. The Contractor shall deliver all Information Technology (IT) Support as defined in this Performance Work Statement (PWS). The Contractor shall ensure that all DCAA-FD users operating in classified space can access network services from their various locations. The Contractor shall report monthly on network reliability, availability, security, and hardware repair and software resolution times. The Contractor shall report monthly on database or application management projects schedule, cost and technical status. The Contractor's performance shall meet or exceed the performance standards detailed in this PWS.

The Contractor shall work closely with military, civilian, and contractor personnel at each location. Because some DCAA-FD employees are located in contractor classified facilities, the contractor shall establish individual working relationships with onsite IT personnel at each location. In some locations, DCAA-FD may have military, civilian or other contractor support performing support. In these cases, the Contractor shall develop and maintain professional relationships to ensure the work is completed and communication is clear. The task objective is for every DCAA-FD employee to have reliable access to DCAA's network equipment, email systems, shared drives and databases, when operating in a classified location.

Services are required on-site at the following operating locations. The Contractor shall ensure an acceptable level of service at all other locations listed in Appendix 2.

- Reston, VA – Desk Side Support, Field Support, and COMSEC Management Services shall be provided
- El Segundo, CA – Desk Side Support shall be provided
- Garland, TX – Desk Side Support shall be provided

3.0 PERFORMANCE REQUIREMENTS

In support of the stated objective, the Contractor shall provide the following Information Technology (IT) Support services:

- Desk Side Support (on-site)

- Field Support
- Communications Security (COMSEC) Management

3.1 Desk Side Support in Sensitive Compartmented Information Facility (SCIF) Locations and Non-Sensitive Locations

If DCAA-FD employee IT problems are not able to be fixed remotely using the DCAA Tier 1 Help Desk, onsite support under this task may be required to solve the problem.

3.1.1 The Contractor shall provide desk side services to support DCAA-FD employees located in SCIF and non-sensitive locations when a remote resolution is not possible or practical. When required, on-site support at the Regional Office (Reston, VA); El Segundo, CA; or Garland, TX will travel to other locations to resolve problems.

3.1.2 The Contractor shall install and maintain Government-owned equipment for DCAA-FD SCIF and non-sensitive locations.

3.1.3 The Contractor shall receive, document, triage, track, and resolve trouble tickets for DCAA-FD in SCIF and non-sensitive locations. DCAA utilizes Microsoft System Center Service Manager (SCSM) as a ticketing system.

3.1.4 The Contractor shall provide customer interface for warrantied hardware trouble tickets in DCAA-FD SCIF and non-sensitive locations. DCAA has hardware warranties on laptops, desktops and miscellaneous other equipment. The Contractor shall work with the hardware vendor and customer to setup dispatch to the site to fix warrantied hardware problems.

3.1.5 The Contractor shall provide basic remote office LAN and WAN hardware installation for all locations. No configuration will be done by the Contractor unless directed to by the Government. However, the Contractor shall assist the engineer with physical troubleshooting, if necessary.

3.1.6 The Contractor shall swap user data, track, plan, configure, and install new computers for DCAA users. The DCAA Regional Office generally receives one shipment of 100 to 250 computers a year. The Contractor shall prepare these computers for shipment to the appropriate offices at Government expense.

3.2 Field Support

The Contractor shall ensure physical support presence at the Regional Office location to respond to any server or WAN issues. This can be deviated from in special circumstances, with Government approval in advance and in writing if, for example, the Contractor is traveling to off-site locations.

Government Regional Information Technology Administrators (RITAs) reserve the right to coordinate or directly assign work priorities to Contractor personnel in case of an emergency or

when attempts to reach the Contractor's PM are unsuccessful. The RITA will follow up with the Contractor's PM via email.

The Contractor shall work with the Government to define regularly scheduled maintenance times which will provide the least impact to the Government's workforce. The Contractor shall adhere to applicable industry standards and maintenance levels for preventative and remedial maintenance. Scheduled maintenance shall consist of server reboots, backups, restores, hardware technical refresh, and software upgrades/patches during non-core hours as per agreed upon timeframes with other on-site contractors and DCAA personnel. On-site support is usually not required, so the majority of the tasks can be done remotely.

In support of this requirement, the Contractor shall:

3.2.1 Provide support for WAN infrastructure. Contractor field support shall not have command line access to any WAN infrastructure.

3.2.1.1 Act as a liaison for the WAN team (composed of contractors under a separate contract), if an onsite person is needed. The Contractor shall maintain a list of contacts to call at each site.

3.2.1.2 Verify power to WAN infrastructure as a first line of troubleshooting.

3.2.1.3 Coordinate with remote site POCs to isolate issues related to a circuit outage, equipment failure or demarcation extension.

3.2.1.4 Provide first level diagnosis for circuit outages. Contractor shall call in circuit outages to the telecom contractor and follow up to get outages restored. If the telecom contractor indicates it is a DCAA's issue, the Contractor shall facilitate getting an alternate form of connectivity (i.e. wireless broadband attached to a laptop) and a console cable connected to the possible defective router so the network team can connect to the router remotely.

3.2.1.5 Replace and install routers, router interfaces, switches, wireless controllers, and wireless access points for network engineering team. The Contractor shall work with the network engineering team to replace defective equipment or to upgrade to new equipment as needed for the site.

3.2.2 Maintain, install, configure, and monitor Microsoft Server Software for field servers. There are approximately 60 field servers.

3.2.2.1 Respond to major server issues (such as crashes, the DHCP stops working, server is not responding), within 20 minutes of problem, during business hours.

3.2.2.2 Fix software or OS issues in one business day; hardware issues shall be fixed within one business day after receipt of replacement part(s).

3.2.2.3 Review disk usage tools to ensure no hard drives exceed 90% capacity.

3.2.2.4 Review Continuity of Operations (COOP) reports to ensure successful replication of data transfers.

3.2.2.5 Respond to Tier II trouble tickets related to any server related actions, including server patches that cannot be installed by SCCM.

3.2.2.6 Ensure all field servers are rebooted each month 10 days after Microsoft "Patch Tuesday". This requires weekend work once per month.

3.2.2.7 Ensure new server hardware is installed and configured with the basic operating system within 20 duty days of receipt. Ensure new server installations meet IAVA compliance before distribution.

3.2.3 Monitor, install, configure, and maintain backup software and Distributed File System Replication (DFSR) for field server backups. DCAA currently utilizes Symantec Backup Exec software

3.2.3.1 Configure and monitor all backup jobs to ensure weekly full backups, and daily differentials for any server where user data changes daily.

3.2.3.2 Maintain backups according to industry best practices, unless otherwise directed by Government

3.2.3.3 Install updates to backup remote agents, when directed by the Government

3.2.3.4 Review DFSR Health reports to ensure nightly replication of data transfers between Regional servers and Region COOP sites are successful

3.2.4 Install, configure, monitor, and maintain required configurations for Microsoft Infrastructure Technology. The Microsoft Infrastructure Technologies include, but are not limited to, Dynamic Host Configuration Protocol (DHCP), Internet Information Server (IIS), Distributed File System Replication (DFSR), File and Print Services, Hyper-V virtual services

3.2.4.1 Technologies must be available during business hours.

3.2.5 Provide required support for Information assurance requirements:

3.2.5.1 Work with the Government’s cyber security branch, as required, to ensure requirements are satisfied

3.2.5.2 Monitor ACAS Security Center daily to identify and resolve any systems requiring adjustments.

3.2.6 Maintain objects for Active Directory:

3.2.6.1 Be responsible for all Active Directory (AD) objects (users, groups, computers, etc.) in the appropriate Regional Organizational Units (OU). Add, modify, and delete objects to keep accurate accountability.

3.2.7 Provide assistance and recommendations for new office setups, office moves, and office closures.

3.2.7.1 Advise Government representative Regional Information Technology Administrator (RITA) on LAN layout in planned new space.

3.2.7.2 Install and test LAN equipment.

3.2.7.3 Troubleshoot user and printer connection issues subsequent to moves to identify cause of problems

3.2.8 Configure, update, and troubleshoot network related problems for printers and multi-function printer for the DCAA enterprise.

3.2.8.1 Configure network printers; apply updates in response to IAVAs;

3.2.8.2 Troubleshoot connectivity and authentication issues on leased and Government- owned network printers.

3.2.8.3 Work with leasing contractor personnel to install leased MFPs on network, and verify CAC authentication.

3.2.9 Provide weekly review for DCAA Dashboards.

3.2.9.1 Review DCAANET Computer Dashboard weekly

3.2.9.2 Review User Dashboard weekly

3.2.10 The Contractor project manager (PM) or designee shall participate in weekly meetings with RITA.

3.3 COMSEC Management Services

The Contractor shall provide Communications Security (COMSEC) management services for classified systems to include Government Guest systems within DCAA-FD. The DCAA-FD will provide workspace on-site at or near the DCAA-FD Regional Office in Reston, VA.

3.3.1 The Contractor shall provide DCAA-FD COMSEC management, support and accountability for all COMSEC equipment and services at all DCAA-FD CONUS sites. The Contractor shall utilize the NSA 3-16 along with sponsoring Agency policies or any subsequent COMSEC NSA documentation.

NOTE: DCAA-FD has over 45 sites that contain COMSEC materials that consist of secure transmission devices to include KSV-21 Enhanced Crypto Cards, Secure DTD2000 System (SDS), Gateway Fax Systems (GWFS), and Type 1 Encryption Devices TACLANES (KG-175). The Contractor shall support DCAA-FD on COMSEC duties at all DCAA-FD sites nationwide. DCAA-FD has Government Guest systems that contain COMSEC equipment, such as TACLANES.

3.3.2 The Government will assign the Contractor as a COMSEC user for Two-Person Integrity (TPI) on handling and destroying COMSEC aids.

3.3.3 The Contractor shall key/re-key secure transmission devices when required. The Contractor shall perform inventory of the devices at the DCAA-FD location.

3.3.4 The Contractor shall be responsible for the receipt, custody, issue, safeguarding, accounting, and when necessary, destruction of COMSEC material.

3.3.5 The Contractor shall be responsible for the maintenance of up-to-date records and the submission of all required accounting reports, which include submitting transfer, inventory, destruction, and possession reports.

3.3.6 The Contractor shall establish a recurring training program designed to ensure all COMSEC users are thoroughly familiar with NSA 3-16 along with sponsoring Agency policies for handling and destroying COMSEC aids, identifying and reporting incidents, and proper COMSEC equipment use. The Contractor shall conduct and document training semiannually.

3.3.7 The Contractor shall provide the Regional COMSEC Officer (RCO) and DCAA with an Account Updated Letter, initially upon location establishment, semiannually thereafter or anytime information contained in the letter changes.

3.3.7.1 The Contractor shall receive, provide receipts for, and ensure the safeguarding and accounting of COMSEC material issued to the COMSEC account and, when applicable, produced within the location.

3.3.8 The Contractor shall maintain COMSEC accounting and related records as outlined in NSA 3-16 along with sponsoring Agency policies and any subsequent changes.

3.3.9 The Contractor shall conduct an inventory semiannually by physically sighting all COMSEC material charged to the account and reconcile this inventory with the Custodian of Record (COR).

3.3.10 The Contractor shall ensure two COMSEC-briefed individuals destroy COMSEC aids as directed in NSA 3-16.

3.3.11 The Contractor shall ensure the integrity of COMSEC material (i.e., key or equipment) and inspect the implemented protective technologies upon initial receipt, during each inventory, and prior to each use.

3.3.12 The Contractor shall ensure the prompt and accurate entry of all amendments to COMSEC publications held by the account.

3.3.13 The Contractor shall ensure that required page check is accomplished on all keying material (as specified in NSA 3-16) and on all publications when they are received, returned from hand receipt, transferred, destroyed, when a change of manager occurs, and when posting amendments which include replacement pages to ensure completeness of each publication.

3.3.14 The Contractor shall ensure all accountable COMSEC material shipped outside of the account's organization is packaged and shipped as specified in NSA 3-16 along with sponsoring Agency policies. The Contractor shall ensure all material received is inspected for evidence of tampering. If the size of the COMSEC account is so large as to prevent the Contractor from personally checking security packaging and markings, the Contractor shall perform page checks and post amendments, and such actions may be performed by other individuals appropriately cleared and authorized provided these individuals are properly instructed by the Contractor. If a suspected physical incident is found, the Contractor shall submit a report immediately to DCAA-FD Security or the designated individual/office.

3.3.14.1 The Contractor shall provide timely response to any DCAA-FD or designated individual/office security queries or tasking.

3.3.14.2 The Contractor shall ensure that appropriate COMSEC material is readily available to properly cleared and authorized individuals whose duties require its use. If the material is classified, the Contractor shall verify that the individuals are cleared to the level of the material. The Contractor shall issue material to users by means of a hand receipt, as provided for in NSA 3-16 along with sponsoring Agency policies and advise recipients of their responsibility for safeguarding the material until it is returned to the DCAA-FD FAO Manager.

3.3.14.3 The Contractor shall report immediately to DCAA-FD Information Systems Security Officer designated individual/office any known or suspected COMSEC incidents, personnel incidents or physical incidents, and submit a report in accordance with the procedures outlined in NSA 3-16 along with sponsoring Agency policies.

3.3.14.4 The Contractor shall verify the identification, clearance and need-to-know of any individual requesting access to the records and/or material associated with the COMSEC account.

3.3.14.5 The Contractor shall support DCAA-FD personnel, as necessary, on new installs, circuit outages, and troubleshooting all COMSEC devices.

3.3.14.6 The Contractor shall submit COMSEC access requests to the RCO on qualified, cleared personnel; conducts COMSEC briefings on approved personnel and debriefing for personnel no longer requiring access; and documents and maintains all requests, briefings and debriefings according to established file plan retention criteria.

3.3.14.7 The Contractor shall maintain a written emergency evacuation and/or destruction plan and ensure all COMSEC-briefed personnel (both Government and contractor personnel) are properly trained on their duties and responsibility within the plan.

3.3.14.8 The Contractor shall initiate and post an accurate list of persons authorized access to the location's COMSEC assets. The Contractor shall obtain the Government's signature on the list prior to posting.

3.3.14.9 The Contractor shall conduct a semiannual or annual COMSEC inventory with the RCO at all DCAA-FD sites where COMSEC assets are located.

3.3.15 The Contractor shall ensure operational COMSEC cryptographic equipment assigned to DCAA-FD locations is filled in accordance with the supporting key's effective date. The Contractor shall load new key upon supersession of the old key or upon inadvertent equipment zeroization.

3.3.16 The Contractor shall create and maintains a COMSEC file plan.

3.3.17 The Contractor shall preserve and/or purge individual file plan records in accordance with specific retention instructions.

3.3.18 The Contractor shall troubleshoot and support STE phones and secure faxes.

4.0 DELIVERY SCHEDULE

The table below delineates requirements and their respective due dates during the performance of this task.

Requirement (PWS reference)	Due Date	Copy to
Kickoff meeting presentation material (9.9)	Kickoff Meeting to be held within five work days after award; presentation material to be provided prior to the meeting	CO, GSA PM and COR
Monthly status reports (11.0)	By the fifth work day of the following month	GSA PM, COR and AASBS
Updated Quality Control Plan (10.1)	Within five work days after award or when there are changes in key personnel or procedures	GSA PM, COR and AASBS
Travel requests and estimate (9.8)	Obtain government authorization prior to each trip for each traveler	GSA PM, COR and AASBS
Labor hours reporting (9.10)	Report all Contractor and subcontractor labor hours no later than October 31 of each calendar year	http://www.ecmra.mil/
Final invoice and Release of Claims (13.5)	No later than 90 days after completion of this task order	AASBS
Phase-in and Phase-out	Updated plan within five calendar days after	GSA PM, COR and

Transition Plan (9.12)	award	AASBS

4.1 Release of Information

Documents developed and maintained in support of this task are not publically releasable and shall be marked with the appropriate distribution statement as directed by the COR.

5.0 SECURITY REQUIREMENTS

The Contractor shall identify qualified personnel possessing the requisite security clearance, per Intelligence Community Directive (ICD) 704, Subject: Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Controlled Access Program Information, and security standards needed for access into the classified area facility and for performing the scope of work covered by the PWS. Advance coordination between authorized security channels, the Program Security Officer (PSO), and COR regarding appropriate clearance and related issues, will be completed prior to Government approval of Contractor personnel being assigned to support this PWS.

The Contractor shall ensure that all personnel are cleared SCI prior to working on this contract. For individuals possessing current accesses, but have outdated Single Scope Background Investigations (SSBIs), the Contractor must show that a Periodic Re-investigation (PR) (SF-86 package) has been submitted to the DCAA-FD Security Office, along with the date it was submitted so that the Government Program Security Office (PSO) can verify the PR is being processed.

The Government will exercise full and complete control over granting, denying, withholding, or terminating security clearances for Contractor employees.

All classified work performed for this effort shall take place within accredited Sensitive Compartmented Information Facility (SCIF) spaces that comply with Intelligence Community Directive (ICD) 705, Subject: Sensitive Compartmented Information Facilities, approved physical, technical, and communications guidelines. Any exception to this requirement will require prior approval from the Government PSO.

The Contractor personnel shall follow site rules and regulations and must take mandatory site-specific security training in accordance with Government policies and guidelines.
All system administrators (privilege users) will be subject to a yearly counter-intelligence (CI) polygraph in order to perform system/network administration functions and maintain privileged user status/access.

All Contractor support personnel shall hold a Top Secret (TS) clearance with a favorably adjudicated Single Scope Background Investigation (SSBI) for Sensitive Compartmented Information (SCI) eligibility. All SCI, Special Access Program (SAP), and COMSEC briefings will be coordinated with the DCAA-FD Chief, Security Division (FDSD), along with the appropriate customer. Contractor personnel will be subject to counterintelligence (CI) polygraph exams, random drug testing, and annual SF 86C submissions.

All mandatory specialized training shall be at Contractor's expense. Contract employees will be removed from the contract for failure to meet and maintain training and certification requirements. Training conducted after employee start date shall not be during duty hours.

6.0 CONTRACTOR IDENTIFICATION

Contractor personnel shall identify themselves as a contractor when attending meetings, answering government telephones, sending and replying to emails, or where their contractor status is not obvious to third parties (i.e., e-mail). The Contractor shall mark any documents as being contractor-prepared or ensure that its participation as a contractor is appropriately disclosed.

7.0 PROPRIETARY/SENSITIVE DATA REQUIREMENTS

The data processed within DCAA offices is considered proprietary and/or sensitive and therefore cannot be used to solicit or benefit other work by the Contractor. All personnel assigned to perform work associated with this contract shall be required to sign a non-disclosure of proprietary or sensitive information agreement and is subject to the security requirements of the performance work statement.

All records received, created, used, and maintained by the Contractor for this effort shall be protected as sensitive data, in accordance with Government laws, to include the Federal Acquisition Regulation (FAR) Part 24 and shall be returned and provided to the Government upon contract completion. Records shall be maintained in accordance with the DCAA Manual 5015.1, Files Maintenance and Disposition Manual.

All data created for Government use and delivered to, or falling under the legal control of the Government are Federal records and shall be managed in accordance with records management legislation as codified at 44 U.S.C. Chapters 21, 29, 31, and 33, the Freedom of Information Act (5 U.S.C. 552), and the Privacy Act (5 U.S.C. 552a), and shall be scheduled for disposition in accordance with 36 CFR 1228.

As prescribed in FAR 24.104, under the Privacy Act Notification Clause (Apr 1984) the Contractor shall comply with clauses 52.224-1 and 52.224-2.

The DCAA PM will specify the delivery to the Government of all data needed for the adequate and proper documentation of contractor-operated programs in accordance with record keeping requirements of 36 CFR Chapter 12, section 1222.48 and with requirements of the FAR and, where applicable, the Defense Federal Acquisition Regulation Supplement (DFARS).

8.0 INFORMATION ASSURANCE CONTRACTOR TRAINING AND CERTIFICATION

The Contractor shall ensure that personnel accessing information systems have the proper and current information assurance certification to perform information assurance functions, in

accordance with DoD 8570.01-M, Information Assurance Workforce Improvement Program, which can be found at: http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf. The Contractor shall meet the applicable information assurance certification requirements, including DoD-approved information assurance workforce certifications appropriate for each category and level, as listed in the current version of DoD 8570.01-M. In support of this requirement, the Contractor shall possess:

8.1 Appropriate operating system certification for information assurance technical positions, as required by DoD 8570.01-M, and maintain Continuing Professional Education (CPE) requirements

8.2 Upon request by the Government, the Contractor shall provide documentation supporting the information assurance certification status of personnel performing information assurance functions

8.3 Contractor personnel who do not have proper and current certifications shall be denied access to DoD information systems; therefore, these credentials shall be in place before Contractor employees are assigned to perform PBSOW functions

8.4 All mandatory specialized training noted shall be at the Contractors expense. Contract employees will be removed from the contract for failure to meet training and certification requirements within the specified timeframe. Training conducted after employee start date shall not be during duty hours. The following Technical Professional Certificates are required to successfully fulfill the mission requirements of this task order:

8.4.1 Field Support requires a minimum IAT Level 2 security certification and Microsoft MTA (IT Infrastructure Track)

8.4.2 Desk Side Support is required to obtain at a minimum IAT Level 1 security certification or higher and entry level Microsoft Windows certification or higher.

8.5 The Contractor shall maintain the currency of their employees by providing initial and refresher training, as required, in order to meet the PBSOW requirements. The Contractor shall maintain a record of all required training and certifications for personnel, and grant the Government access to these records, upon request.

8.5.1 The Contractor shall attend Government-provided specialized training (i.e., not commercially available), as required. The Government will provide initial training for new or modified systems for which commercial training is not available.

8.5.2 The Contractor shall comply with all of DCAAs internal compliance training requirements for contractors.

8.5.3 The Contractor shall refund to the Government training and education costs provided by the Government to Contractor employees who resign within 12 months of completion of such training, unless the departure was directed by the Government.

9.0 GENERAL REQUIREMENTS

9.1 Period of Performance

The period of performance consists of a base period starting in September 2015 (or as soon as possible) through March 31, 2016, plus four one year options.

9.2 Location and Hours of Work

The Contractor is responsible for conducting business during DCAA operating hours, Monday thru Friday except Federal holidays or when the supported facility is closed due to local or national emergencies, administrative closings, or similar directed facility closings. System maintenance, backup and upgrades will occur at pre-defined non-core hours. The Contractor shall work with the government to define regularly scheduled maintenance times which will provide the least impact to the government's workforce.

Accomplishment of the tasks contained in this PWS requires work at the locations specified in paragraph 1.0 and at various contractor, subcontractor, and Government facilities (mainly in the continental United States)

9.3 Government-furnished Equipment and Materials

The Government shall furnish onsite desk, chair, and computer equipment with internet access, telephone, facsimile machine, copy machine, and use of office supplies as deemed reasonable by the DCAA PM for the effort, as required. The equipment issued shall be IAW DoD and DCAA policies and shall be used only for the performance of this performance work statement and shall not be used for personal use.

9.4 Non-Personal Services

This is not a personal services contract. The Government shall neither supervise contractor employees nor control the method by which the contractor performs the required tasks. It shall be the responsibility of the Contractor to manage its employees and to guard against any actions that are of the nature of personal services, or give the perception of personal services. If the Contractor believes that any actions constitute, or are perceived to constitute personal services, it shall be the Contractor's responsibility to notify the Contracting Officer immediately.

9.5 Business Relations

The Contractor shall successfully integrate and coordinate all activity needed to execute the requirement. The Contractor shall manage the timeliness, completeness, and quality of work performed. The Contractor shall provide corrective action plans, proposal submittals, timely identification of issues, and effective management of subcontractors. The Contractor shall ensure professional and ethical behavior of all contractor personnel.

9.6 Task Management

The Contractor shall establish clear organizational lines of authority and responsibility to ensure effective management of the resources assigned to the requirement. The Contractor shall maintain continuity between the support operations at DCAA-FD locations and the Contractor's corporate offices.

9.7 Personnel Administration

The Contractor shall maintain the currency of their employees by providing initial and refresher training as required to meet the PWS requirements. The Contractor shall make necessary travel arrangements for employees.

The Contractor shall accomplish the assigned work by employing and utilizing qualified personnel with appropriate combinations of education, training, and experience.

9.8 Travel

The DCAA PM/COR will determine when travel is needed. The Contractor shall comply with the Federal Travel Regulation (FTR) in requesting approval and providing a cost estimate in advance of each trip and billing the Government in a timely manner after the completion of each trip.

Prior to each trip, the Contractor shall complete the DCAA Form 5000-8, DCAA Contract Travel Authorization/Reimbursement, and show the estimated travel costs. The completed form shall be submitted to the DCAA PM/COR for review and approval. Failure to obtain pre-approval may result in rejection of the Contractor’s invoice for travel charges.

Upon completion of travel, the Contractor shall provide a completed DCAA Form 5000-8 showing the actual travel costs to the DCAA PM/COR. The completed form shall also accompany the Contractor’s invoice for travel along with copies of receipts for transportation, lodging and all charges over $75. Only allowable and authorized travel charges shall be billed to the Government. Refer to FAR 31.205-46 regarding allowable travel costs. The Contractor shall maintain a file of all approved travel authorizations and copies of all supporting documentation submitted for reimbursement of travel costs.

Local travel shall be at the Contractor’s expense and shall not be billable to the Government.

9.9 Kickoff Meeting

The Contractor shall attend the joint Government and Contractor kickoff meeting to review PWS requirements and provide a briefing on the Contractor’s Quality Control Plan and Staffing Plan within five (5) work days after contract award.

9.10 Contractor Reporting Requirements

The Contractor shall report ALL Contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the Defense Contract Audit Agency via a secure data collection site. The Contractor is required to completely fill in all required data fields using the following web address: http://www.ecmra.mil/

Reporting inputs will be for the labor executed during the period of performance during each Government fiscal year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year, beginning with 2013. Contractors may direct questions to the help desk at: http://www.ecmra.mil.

9.11 Contractor Furnished Items and Services

Unless otherwise stated in this PWS as Government-furnished, the Contractor shall provide all facilities, labor, equipment, supplies, management oversight, and administrative support necessary to successfully fulfil the requirements herein.

9.12 Phase-in and Phase-out Transition Plan

The Phase-In and Phase-Out processes are defined as smooth transitions from one contractor to another to maintain the program integrity required under the contract. The Contractor shall take all actions necessary to achieve a successful transition from the incumbent contractor for the phase-in process and to the follow-on contractor for the phase-out process. The Contractor shall maintain full contract compliance during the period of time leading up to contract expiration or termination.

The Contractor shall submit an updated Phase-in and Phase-out Transition Plan within five calendar days after contract award. This plan shall address the following:

- Transition Team
- Risks and contingencies
- Strategies and tools
- Transition schedule and activities
- Reporting and communication procedures
- Management controls

The Contractor shall coordinate its phase-out activities with the incoming Contractor to effect a smooth and orderly transition at the end of the contract period. The Contractor shall provide, through the authorized Government representative, records and information related to the services performed under this task. The Contractor shall remove all Contractor-owned property from the Government spaces or facilities by close of business on the last day of the contract.

10.0 QUALITY CONTROL AND ASSURANCE

10.1 Quality Control Plan

The Contractor shall develop and maintain an effective quality control program to ensure services are performed in accordance with this PWS. The Contractor's quality control program is the means by which the Contractor assures itself that all work complies with the requirements described in the PWS. The Contractor shall develop and implement procedures to identify and prevent defective services and ensure the non-recurrence of such services. The Contractor shall apply industry standards and best practices to include, at a minimum, identification of quality control factors and processes, evaluation methods, performance monitoring and process improvement. The Contractor shall develop a contingency plan to ensure acceptable deliverables are submitted on time.

The Contractor's Quality Control Plan (QCP) shall describe a process that supports the execution of this task as delineated in this PWS. The QCP shall include inspection, validation, evaluation, corrective action and procedures necessary to affect quality control of all performance and products under this task in accordance with the Government's Quality Assurance Surveillance Plan (QASP) in Appendix 5. The QCP shall include an inspection system covering all the performance evaluation attributes. It must specify the areas to be inspected on a scheduled and unscheduled basis, how often inspections shall be accomplished, the title of the individual(s) who shall perform the inspection, and the methods for identifying and preventing defects in the quality of services. The Contractor shall allow inspection and evaluation by the Government throughout the task period. Records of all inspections conducted by the Contractor and necessary corrective action taken shall be made available to the Government during the term of the task.

The Contractor shall provide a revised, updated QCP within five work days after award or when there are changes in key personnel or procedures.

10.2 Quality Assurance Surveillance Plan (QASP)

The Government is responsible for administering this contract and overseeing and evaluating the Contractor's performance. This Quality Assurance Surveillance Plan (QASP) has been developed to evaluate Contractor actions while implementing this PWS. It is designed to provide an effective surveillance method of monitoring Contractor performance for each listed requirement. The Government will evaluate the Contractor as described in Appendix 5.

11.0 MONTHLY STATUS REPORT (MSR)

The Contractor shall prepare and submit monthly status reports delivered in a format and/or media approved by the GSA Project Manager. These managerial reports shall include the following elements:

- Contractor's name and address
- Contract number, Order number, ACT number, Task Order ID number
- Contract line item number (CLIN) (and SubCLIN number if applicable)
- Date of report
- Period covered by report
- Description of services provided during report period, including problem areas encountered, and recommendations, if any, for solutions. Recommendations may include

solutions outside the scope of this contract.
- Travel completed during the reporting period, including estimated cost for each trip.
- Plans and recommendations for activities, including travel, during the next reporting period

The MSRs shall contain the following specific information related to Section 3.0 services..

11.1 Monthly reporting of desk side support statistics.

11.2 Status of COMSEC account to include inspections conducted with results and any COMSEC related security incidents.

12.0 POINTS OF CONTACT

12.1 DCAA Client Representative/Project Manager

Ms. Diane Reid
Contract Manager
DCAA
8725 John J. Kingman Road, Suite 2135
Fort Belvoir, VA 22060
(b) (6)
Email: Diane.Reid@dcaa.mil

The DCAAs Headquarters Information Technology Division is designated as the Project Manager (PM) for this effort. The DCAA PM will oversee the Contractor's services in accordance with the PWS and be responsible for review and approval of all technical services and deliverables in coordination with the DCAA COR. The Project Manager will serve as the Quality Assurance Evaluator (QAE) and assist the COR with vendor performance evaluation against the tasks in this contract.

12.2 GSA Project Manager (PM)

Paul Cook
Technology Project Executive
GSA, FAS, Assisted Acquisition Services Division (9QFAD)
(b) (6)
Fax: 520-296-1183
Email: paul.cook@gsa.gov

The GSA PM is responsible for overseeing the Contractor's overall technical performance and responding to matters of a technical nature. This person will be the Contractor's primary point of contact for resolving technical issues.

12.3 GSA Administrative Contracting Officer (ACO)

Jo Ann Lew
Sr. Contracting Officer
GSA, FAS, Acquisition Operations Division (9QZAA)
50 United Nations Plaza, 2nd Floor, Room 2426
San Francisco, CA 94102-4912
(b) (6)
Fax: 415-522-4545
Email: joann.lew@gsa.gov

The GSA ACO is responsible for the award and administration of this contract. All responsibilities not delegated to the COR or performed by the GSA PM remain within the purview of the GSA ACO. Any changes and non-technical questions should be brought to the attention of the GSA ACO.

13.0 PAYMENT PROCEDURES

13.1 GSA Electronic Invoicing

All invoicing shall be done electronically. Password and electronic invoice access may be obtained through the GSA Finance website at www.finance.gsa.gov and the AASBS Portal web site at https://portal.fas.gsa.gov/web/guest

The Contractor shall upload invoices into the AASBS Portal and the GSA Finance website. The COR will review invoices in the AASBS Portal within three (3) work days of receipt and notify the GSA PM of the results of its review. If the invoices are acceptable, then the GSA PM will approve them for payment and complete the information in the AASBS portal (this information is transmitted to GSA Finance as a receiving report to be matched to the Contractor's invoice for payment purposes). If the COR finds the invoice to be unacceptable, the COR will notify the GSA PM, who will either reject the invoice or discuss the matter with the Contractor.

13.2 Payment Schedule

The Contractor may submit monthly invoices. The billing period shown on each monthly invoice shall be for a calendar month, i.e., September 1 through 30, 2015. If the task begins after the first of the month, then the charges for the first and last months of the task shall be prorated. For example, a monthly charge of $5,000 for the period of September 10 through 30, 2015, shall be billed at $3,500 ($5,000 x 0.7000). Appendix 6 shows factors to be used for prorating monthly charges.

13.3 Invoice Requirements

At a minimum, the following information must be included on each invoice.

(a) Contractor's name, "remit to" address, and contact information. The "remit to" address must correspond to the payment address shown on the order.
(b) Contract number, order number, task number, and ACT number.

(c) Invoice number, date, and billing period
(d) Item numbers, charges, subtotal, credits, deductions, and total

Also refer to the "Contractor's invoice" requirements contained in FAR 52.232-25. Failure to submit a proper invoice may result in either a partial payment or rejection of the invoice.

13.4 GSA AAS Business Systems (AASBS) Portal

The GSA AASBS Portal will be accessible to the Client Representative and Contractor during the performance of this order and shall be used in the administration of this order. This web-based system at https://portal.fas.gsa.gov/web/guest shall be used by the Contractor to upload monthly status reports, deliverables, and invoices and to respond to inquiries. The Contractor shall maintain a current account on this system.

13.5 Contractor's Final Invoice and Release of Claims

The Contractor's final invoice for this task must be so identified and submitted after the task has been completed and no further charges are to be billed. The final invoice shall be submitted no later than 90 days after completion of this task order.

The Contractor shall comply with FAR Clause 52.212-4, paragraph (i), subparagraph (7), and submit a signed and executed Release of Claims with the final invoice.

Appendix 1 – Acronyms

AASBS	-	Assisted Acquisition Services Business Systems
ACAS	-	Assured Compliance Assessment Solution
AD	-	Active Directory
AQL	-	Acceptable Quality Level
APPS	-	Audit Planning and Performance System
CAC	-	Common Access Card
CFR	-	Code of Federal Regulations
CI	-	Counter-Intelligence
COMSEC	-	Communications Security
CONUS	-	Continental United States
COOP	-	Continuity of Operations
COR	-	Contracting Officer's Representative or Custodian of Record
COTS	-	commercial-off-the-shelf
CPE	-	Continuing Professional Education
DCAA	-	Defense Contract Audit Agency
DCAANET	-	DCAA Network
DFARS	-	Defense Federal Acquisition Regulation Supplement
DFSR	-	Distributed File System Replication
DHCP	-	Dynamic Host Configuration Protocol
DMIS	-	DCAA Management Information System
DoD	-	Department of Defense
eCMRA	-	Enterprise-wide Contractor Manpower Reporting Application
FAO	-	Field Audit Office
FAR	-	Federal Acquisition Regulation
FAS	-	Federal Acquisition Service
FD	-	Field Detachment
FDSD	-	Field Detachment Security Division
FOUO	-	For Official Use Only
FLA	-	Financial Liaison Advisor
FTR	-	Federal Travel Regulation
GFE	-	Government Furnished Equipment
GOTS	-	government off the software
GSA	-	General Services Administration
GWFS	-	Gateway Fax System
IAT	-	Information Assurance Technical
IAVA	-	Information Assurance Vulnerability Alert
IAW	-	in accordance with
ICD	-	Intelligence Community Directive
IIS	-	Internet Information Server
IT	-	Information Technology
LAN	-	Local Area Network
MER	-	Master Employee Record
MFD	-	Multifunction Device
MFP	-	Multifunction Printer

MS	-	Microsoft
MSR	-	Monthly Status Report
NCSM	-	Network Communications Security Manual
MTA	-	Microsoft Technology Associate
NSA	-	National Security Agency
OS	-	Operating System
OU	-	Organizational Unit
PM	-	Project Manager
POC	-	Point of Contact
PR	-	Periodic Re-investigation
PSO	-	Program Security Officer
PWS	-	Performance Work Statement
QCP	-	Quality Control Plan
QAE	-	Quality Assurance Evaluator
RITA	-	Regional Information Technology Administrator
RCO	-	Regional COMSEC Officer
SAP	-	Special Access Programs
SAAR	-	System Authorization Access Request
SCCM	-	System Center Configuration Manager
SCI	-	Sensitive Compartmented Information
SCIF	-	Sensitive Compartmented Information Facility
SCSM	-	System Center Service Manager
SDS	-	Secure DTD2000 System
SSBI	-	Single Scope Background Investigation
STD	-	Standard
STE	-	Secure Terminal Equipment
STIG	-	Security Technical Information Guidance
TACLANE	-	Tactical Local Area Network Encryption
TPI	-	Two-Person Integrity
TS	-	Top Secret
USC	-	U. S. Code
VA	-	Virginia
WAN	-	Wide Area Network

Appendix 2 – DCAA Locations and Estimated Number of Employees

Office Code	Office City	Office State	Office Zip	# Employees *
09712	Reston	VA	20190	9
09883	Ashburn	VA	20166	8
0976D	Aurora	CO	80011-9046	3
09011	Centreville	VA	20120-2290	3
09012	Centreville	VA	20120-2290	2
09851	Chantilly	VA	20153	4
09852	Chantilly	VA	20153	4
09013	Ft. Belvoir	VA	22060-6219	4
09741	Garland	TX	75046-1283	4
09742	Garland	TX	75046-1283	16
09891	Greenville	TX	75403-6056	4
09892	Greenville	TX	75403-6056	18
09841	El Segundo	CA	90251	4
09842	El Segundo	CA	90251	5
09884	Herndon	VA	20191	1
09885	Herndon	VA	20171	2
09821	King of Prussia	PA	19406	4
09822	King of Prussia	PA	19406	29
0976C	Las Vegas	NV	89119	2
09771	El Segundo	CA	90260-0668	4
09861	El Segundo	CA	90260	5
09862	El Segundo	CA	90260	22
09871	Linthicum	MD	21090-0089	5
09872	Linthicum	MD	21090-0089	19
09767	Littleton	CO	80127-0094	5
09721	Merrimack	NH	03054-2063	4
09811	Merrifield	VA	22116	4
09812	Merrifield	VA	22116	19
0977A	Palmdale	CA	93599	6
09845	Placentia	CA	92871-0515	5
09711	Reston	VA	20195-8726	5
09731	Rochester	NY	14617-0290	4
09732	Rochester	NY	14617-0290	15
09775	San Diego	CA	92198-0274	4
09779	San Diego	CA	92121	6
09847	Seattle	WA	98023	1
09846	St Louis	MO	63134	3

Office Code	Office City	Office State	Office Zip	# Employees *
09761	Sunnyvale	CA	94088-0277	5
09762	Sunnyvale	CA	94088-0277	6
09844	Westminster	CA	92684-4242	6
09311	McLeansville	NC	27301	5
09312	McLeansville	NC	27301	13
09873	Annapolis	MD	21409-6107	1
09313	Orlando	FL	32819-8909	3
0971B	Fair Lakes	VA	22033-4232	4
09314	Melbourne	FL	32906	17
09723	Hudson	NH	03051-5244	10
09725	Danbury	CT	06810-7589	4
09724	Andover	MA	01810-1021	8
09858	Fair Lakes	VA	22033-4232	5
09859	Laurel	MD	20723	5
09321	Huntington Beach	CA	92647	7
0971C	Sterling	VA	20166	6
09778	Redondo Beach	CA	90278	8
09886	Ashburn	VA	20166	9
09881	Ashburn	VA	20166	3
0985A	Fair Lakes	VA	22033	8
09014	Reston	VA	20192	7
09015	Reston	VA	20192	1
09016	Reston	VA	20192	13
09017	Reston	VA	20192	11
09018	Reston	VA	20192	1
09019	Reston	VA	20192	7
09816	Arlington	VA	22201	1
Estimated Total				436

Appendix 3 – Estimated Quantity and Description of Requirements

DESKTOP EQUIPMENT SUMMARY

System	2015	2016	2017	2018	2019
Laptop/Desktop Computers	900	950	975	1000	1025
Servers	60	65	65	70	70
Networked Printers/MFP	100	105	110	115	120
Non-networked Printers	30	35	40	45	50
Copiers	NA	NA	NA	NA	NA
Personal Scanners	250	275	300	325	350
Number of Images Supported	NA	NA	NA	NA	NA

WORKLOAD VOLUME

Type	Past 12 Months
Tier II Tickets	400-500
Hardware Tickets	500
Installs, moves, adds, changes	200-400 per year
Image Changes	N\A

SUPPORTED HARDWARE AND SOFTWARE

Software Standards	Detail
Standard	See below
Nonstandard	0
Operating System Mix	Any currently Microsoft supported Operating System
Hardware Standards	**Number**
Hardware supported	Include but not limited to: Laptops/Desktop, Blackberries, monitors, port replicators, multi-function printers, printers, keyboards, mice, STE Phones/Secure Fax, LAN/WAN equipment (Routers/switches), Servers, Cryptographic equipment (i.e., TACLANES, SKV)
Business Applications	**Number**
Number of Standard Applications	Include but not limited to: ActivClient; Adobe Connect Add-in Checker; Adobe Flash Player ActiveX; Adobe Flash Player Plugin; Adobe Reader; Adobe Shockwave Player; Apps tools for office; BlackBerry; Cute PDF; Dame Ware Mini Remote control agent; DCAA APPS; DCAAM; DMIS; Excel Power Tools for Office; EZ-Quant; Java Runtime Environment; Juniper VPN Setup Service; McAfee; Microsoft .Net Framework; Microsoft Lync; Microsoft Office; Microsoft Silverlight; Open Text Enterprise Connect; Oracle Instant Client; Oracle jinitiator; QARRS; Roxio Create NXT Silver; WinZip; WS_FTP;

	Symantec Backup Exec, COGNOS, IMPROMPTU/PowerPlay; Microsoft Infrastructure Technologies include, but are not limited to, Dynamic Host Configuration Protocol (DHCP), Internet Information Server (IIS), Distributed File System Replication (DFSR), File and Print Services, Hyper-V virtual services

Appendix 4 – Service Level Metrics

1. First Call Resolution:

Description: Percentage of user incidents that are resolved by the desk side support. Note: a "user incident" would be an incident initiated by a user (as opposed to a ticket initiated by IA, a ticket created by a tech documenting a configuration change, server installation, etc.)

Formula: (# of Service-desk resolved user incidents) / (# of user incidents) * 100
Measured: Monthly
Reasonable AQL: 60%

2. Incorrectly Assigned Incidents:

Description: If an incident cannot be resolved by the desk side support, it must be assigned to one of the Tier 2 groups. This measures the percentage of incorrectly assigned tickets versus all resolved tickets.

Formula: (# of escalated incidents improperly assigned) / (# of escalated incidents resolved) * 100
Measured: Monthly
Reasonable AQL: <5%

3. Percentage of overdue service requests

Description: This tracks the number of service requests that are not completed within the customer-required time frame.

Formula: (# of service requests not completed within timeframe) / (# of service requests completed) * 100
Measured: Monthly
Reasonable AQL: <10%

(Note: this implies that you should establish time frames for service requests separate from incidents)

4. Percentage of abandoned calls

Description: This tracks the percentage of abandoned calls that were not handled by the desk side support. Note: in order to screen out hang-ups, wrong numbers, and people who get what they need from an automated announcement, it is best to place a minimum time on a "valid" call -- we call those "true call abandonments"

Formula: (# of true call abandons) / (# of calls) *100
Where: True Call Abandon = calls abandoned after being on hold for 60 seconds
Measured: Monthly

Reasonable AQL: <5%

5. Average call hold time for completed calls

Description: This measures how long a user is on hold before being helped. Generally, the longer a person is on hold, the angrier they will be.

Measurement: (Cumulative Hold Time for Completed Calls) / (Number of Completed Calls)
Measured: Monthly
Reasonable AQL: <5 minutes

6. Voicemails
Voicemails must be returned within 15 minutes or a ticket generated with automatic email sent. Voicemails left outside of business hours must be returned during the first 90 minutes of the next business day.

Measured: Monthly
Reasonable AQL: <5 minutes

TROUBLE TICKET TRANSFER AND DISPATCH

1. Calls that cannot be resolved remotely by Tier 1, such as hardware failures, telecommunications, security, loss of Internet or WAN connectivity, etc., shall be transferred to the appropriate Tier 2 support area.

2. Contractor shall transfer trouble tickets to the appropriate support personnel in such a way as to expedite acknowledgement by the dispatched personnel.

3. For calls related to Government developed and supported applications (GOTS), Vendor shall document initial problem determination / isolation and transfer ticket to the appropriate Tier 2 area of support.

4. In the event a caller calls with a question on a non-supported product, the Vendor shall refer the end user to Field Support.

5. Contractor shall coordinate with DCAA management and support staff as necessary during problem resolution.

6. “Warm transfers” shall be used whenever customer calls are moved from one telephone support individual to another.

SERVICE LEVELS

COMMON TERM	Definition
PRIORITY LEVELS	"Priority levels" (or severity levels) are defined categories that identify the degree of business criticality and importance to the

COMMON TERM	Definition	
	organization (the "business impact") of specific incidents, and the associated provider response requirements attributed to any such incident. The following priority level table categories and descriptions apply to all services:	
	Priority Level 1 — Emergency/Urgent *Critical Business Impact* *Less than 2 hours to resolve. (does not include time for external vendor Ex.Telecom Provider to fix a problem)*	The problem has caused a complete and immediate work stoppage affecting a primary business process or a broad group of users such as an entire department, floor, branch, line of business, or external customer. No work-around available. Examples: • An inability to conduct electronic trading • No access to the Internet and e-mail • A major network outage where there is no work-around solution available • A security violation (that is, denial of service, port scanning)
	Priority Level 2 — High *Major Business Impact* *Urgency is High-An issue where the system is functioning but in a severely reduced capacity. Significant impact to business operations and productivity. Less than 2 hours to resolve.*	A business process is affected in such a way that business functions are severely degraded, multiple users are impacted or a key customer is affected. A work-around may be available; however, the work-around is not easily sustainable. Examples: • A major network link outage where there is an alternative; however, the alternative is not sustainable • For an Auditor computer in a state that it can't be used for work productivity • VIP Client/User
	Priority Level 3 — Medium *Moderate Business Impact* *Urgency is Medium/Moderate – Routine support requests that impact a single customer or*	A business process is affected in such a way that certain functions are unavailable to end users or a system and/or service is degraded. A work-around may be available. Non critical but significantly affects a customer's performance or ability to perform work, but services are still operational. Examples: • Telecommunication problem (that is,

COMMON TERM	Definition	
	non-critical software or hardware error. Less than 8 hours to resolve.	excessive network latency) • Machine is down • Issue will escalate to Critical if not addressed
	Priority Level 4 — Low *Minimal Business Impact* *Urgency is Low – The incident does not impede or disrupt business operations or productivity and is an inconvenience, 24 to 48 hours to resolve.*	An incident that has little impact on normal business processes and can be handled on a scheduled basis. A work-around is available. A minor service issue or general inquiry. Standard service request, non-core business function Example: • User requests (for example, a system enhancement) • Peripheral problems (for example, a network printer) • Preventive maintenance • Service request is from a user for support, delivery, information, advice, or documentation. Not a failure in the IT infrastructure

Service Level Goals

Component	Explanation of Component
Definition	Time to resolve problems for hardware, software and system components in the desktop environment that are mission-critical or affect a significant number of end users. The number of hours until resolution (Note: Any resolution time requirements less than four business hours will require "hot" spares).
Requirement	Monday through Friday 0600 - 2000 EST/EDT.
Measurement Range	Priority Level 4 = 24-48 hours 90% of the time Priority Level 3 = Less than 8 Hours 95% of the time Priority Level 1 & 2 = Less than 2 hours 96% of the time
Frequency	Monthly
Calculation Formula	Number of problems resolved within SLA time frame/total number of problems = "service level attained"
Data Sources	Microsoft Service Center System Manager (SCSM) system from organization.

Appendix 5 – Quality Assurance Surveillance Plan

Contract Task or Deliverable	Performance Standard	Method of Surveillance
3.1 Desk Side Service Desk Support at SCIF and non-sensitive locations	Once hardware problem is determined, Contractor has one (1) day to call hardware vendor to schedule replacement.	Monthly Status Reports (MSRs) showing desk side support statistics
3.2.2.1 Respond to major server issues	Begin problem resolution within 20 minutes of notification; no more than one exception of this time limit per quarter.	Customer complaints, random review of Contractor's inspection reports, and MSRs
3.2.2.2 Fix software or OS issues	Fix in one business day	Customer complaints and MSRs
3.2.2.2 Repair hardware	Fix hardware issues in one business day after receipt of replacement part(s)	Customer complaints and MSRs
3.2.2.3 Review disk usage tools to ensure no hard drives exceed 90% capacity	Corrective action taken within 7 days, unless directed not to in writing by Government COR before the 7 days.	Random review of Contractor's inspection reports
3.2.2.4 Review COOP reports to ensure successful replication of data transfers	No more than 2 consecutive replication failures, unless a documented attempt at corrective action was taken. Notify Government of replication failures and recommendations for resolution.	Random review of Contractor's inspection reports and MSRs
3.2.2.5 Respond to Tier II trouble tickets related to any server related actions, to include server patches that cannot be installed by SCCM.	Trouble ticket closed within 24 hours. Notify Government of any unresolved IAVA mitigation issues that cannot be resolved within 24 hours.	Customer complaints and MSRs
3.2.2.6 Monthly reboot of all field servers	Reboot 10 days after Microsoft "Patch Tuesday" one weekend per month	MSR
3.2.3.1 Contractor shall configure and monitor all backup jobs to ensure weekly full backups, and daily differentials for any server where user data changes daily.	No server misses 2 consecutive backups, unless a documented attempt at corrective action was taken. Notify Government of any 2 consecutive backup failures and recommendations for resolution.	Random review of Contractor's inspection reports and MSRs
3.2.3.2 Maintain backups according to industry best practices, unless otherwise directed by Government	No server misses 2 consecutive backups, unless a documented attempt at corrective action was taken.	Random review of Contractor's inspection reports and MSRs
3.2.3.3 Install updates to backup	Installation updates are completed	Monthly Status Reports

Contract Task or Deliverable	Performance Standard	Method of Surveillance
remote agents, when directed by the Government	within 7 days	(MSRs) showing desk side support statistics
3.2.3.4 Review DFSR Health reports to ensure nightly replication of data transfers between Regional servers and Region COOP sites are successful	No greater than 2 consecutive replication failures, unless a documented attempt at corrective action was taken. Notify Government in writing of any 2 consecutive replication failures and recommendations for resolution within 2 hours.	Daily report
3.2.4.1 Technologies must be available during business hours.	Corrective action taken within 30 minutes of identified failure	Customer complaints and MSRs
3.2.5.2 Contactor shall monitor ACAS Security Center daily to identify and resolve any systems requiring adjustments.	Corrective action taken within 24 hours of identified mitigation failure. Notify Government of any IAVA mitigation failures after 48 hours	Random review of Contractor's inspection reports and MSRs
3.2.6.1 Contractor shall be responsible for all Active Directory (AD) objects (users, groups, computers, etc.) in the appropriate Regional Organizational Units (OU). Add, modify, and delete objects to keep accurate accountability.	New user accounts shall be created within 24 hours of SAAR notification. Deactivation of user accounts shall be implemented within 2 hours of SAAR. Modification of user account profile and permissions shall be implemented within 4 hours of authoritative email notification. Modification of user account profile and permissions shall be implemented within 8 hours of Master Employee Record (MER) notification. User objects are removed no later than 45 days after those objects are deactivated within AD. Perform quarterly review of inactive computer objects exceeding 30 days of inactivity. Deactivate computer objects and move to disabled computers OU, using locally-generated scripts. Delete computer	Customer complaints, random review of Contractor's inspection reports and MSRs

Contract Task or Deliverable	Performance Standard	Method of Surveillance
	objects after 45 days. Perform quarterly Group membership audits in coordination with group owner and remove orphaned users within 7 days.	
3.2.8 The Contractor shall configure, update, and troubleshoot network related problems for printers and multi-function printer for the DCAA enterprise.	Configures and meets security safeguards on new printer installs completed within 24 hours Maintain STIG and IAVA compliance within specified time frame, usually not to exceed 15 calendar days from notification.	Customer complaints, random review of Contractor's inspection reports and MSRs
3.2.9.1 Review DCAANET Computer Dashboard weekly	Departure from DoD and DCAA policies will not exceed 5 events in any one week	Weekly reviews and MSRs
3.2.9.2 Review User Dashboard weekly	Departure from DoD and DCAA policies will not exceed 5 events in any one week	Weekly reviews and MSRs
3.3 Receipt, maintenance and destruction of COMSEC material	Timely processing and accurate accountability of COMSEC material from receipt to destruction.	Accounting reports and MSR
3.3 Maintain COMSEC training program	Conduct and document training semiannually.	Random reviews of training records and MSR
3.3 Report known or suspected COMSEC incidents and submit report IAW NS-95.1 version 2.0 NCSM procedures	Timely and complete reporting	Random reviews of incident reports and MSR
3.3 Support of DCAA-FD personnel located at COMSEC sites.	Timely and appropriate responses, including providing information, support, problem resolution, and training.	Customer complaints NTE five per month and MSR
3.3 Conduct inventory of COMSEC assets	Annual or semiannual inventories, as appropriate; accurate and complete in all respects; and updated as needed.	Random reviews of inventories

Appendix 6 – Table of Factors for Partial Month Charges (based on 30-day months)

Date Work Begins	# of Billable Days	Factor	Date Work Ends	# of Billable Days	Factor
1	30	1.00000	1	1	0.03333
2	29	0.96667	2	2	0.06667
3	28	0.93333	3	3	0.10000
4	27	0.90000	4	4	0.13333
5	26	0.86667	5	5	0.16667
6	25	0.83333	6	6	0.20000
7	24	0.80000	7	7	0.23333
8	23	0.76667	8	8	0.26667
9	22	0.73333	9	9	0.30000
10	21	0.70000	10	10	0.33333
11	20	0.66667	11	11	0.36667
12	19	0.63333	12	12	0.40000
13	18	0.60000	13	13	0.43333
14	17	0.56667	14	14	0.46667
15	16	0.53333	15	15	0.50000
16	15	0.50000	16	16	0.53333
17	14	0.46667	17	17	0.56667
18	13	0.43333	18	18	0.60000
19	12	0.40000	19	19	0.63333
20	11	0.36667	20	20	0.66667
21	10	0.33333	21	21	0.70000
22	9	0.30000	22	22	0.73333
23	8	0.26667	23	23	0.76667
24	7	0.23333	24	24	0.80000
25	6	0.20000	25	25	0.83333
26	5	0.16667	26	26	0.86667
27	4	0.13333	27	27	0.90000
28	3	0.10000	28	28	0.93333
29	2	0.06667	29	29	0.96667
30	1	0.03333	30	30	1.00000